



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/483,186

01/14/2000

Francisco Corella

10001559-1

8070

22879

7590

07/14/2006

HEWLETT PACKARD COMPANY  
P O BOX 272400, 3404 E. HARMONY ROAD  
INTELLECTUAL PROPERTY ADMINISTRATION  
FORT COLLINS, CO 80527-2400

EXAMINER

BROWN, CHRISTOPHER J

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 07/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/483,186	<b>Applicant(s)</b> CORELLA, FRANCISCO	
	<b>Examiner</b> Christopher J. Brown	<b>Art Unit</b> 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 4/13/06.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>4/13/06</u> . | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Response to Arguments***

Applicant's arguments with respect to claims 1-28 have been considered but are moot in view of the new ground(s) of rejection. Applicant's arguments in regards to the USC 103 rejection of claims 1-28 is moot in view of the new grounds of rejection containing Smith US 6,651,166

Applicant's arguments filed 4/13/06 have been fully considered but they are not persuasive. Applicant argues that it is not inherent in a PKI system that a certificate or ticket is signed. The examiner maintains this rejection on the basis that the entire definition in Newton's Telecom Dictionary (previously cited) includes a certificate authority signing a digital certificate. The examiner suggests that the applicant change "Public Key Infrastructure" (PKI) to Public Key System, Unsigned Public Key Infrastructure or a similar term. This change would overcome the current 112 rejection.

***Claim Objections***

The examiner notes in Claims 1, and 13 that the claims state “at least one of revoked by the certificate authority...”. It appears that the word “of” should be “is” or that some words are missing.

***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-28 are rejected The meaning of every term used in any of the claims should be apparent from the descriptive portion of the specification with clear disclosure as to its import; and in mechanical cases, it should be identified in the descriptive portion of the specification by reference to the drawing, designating the part or parts therein to which the term applies. A term used in the claims may be given a special meaning in the description. No term may be given a meaning repugnant to the usual meaning of the term. See MPEP 608.01 (o).

As per claims 1-28 the term “PKI” is stated in the claims along with unsigned documents. It is inherent in a PKI system that the certificate, or ticket is signed. It is part of the definition Newton’s Telecom Dictionary “....procedures for the distribution of public keys via digital certificates signed by Certificate Authorities....”

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**3. Claims 1, 2, 6, 7, 8, 13, 14, 18, 19, 20, 25, and 26 are rejected under 35 U.S.C.**

**103(a) as being unpatentable over Smith US 6,651,166 in view of “How PGP works”  
in view of Fischer US 5,475,826**

As per claims 1, 13, 25, and 26 Smith teaches a certificate authority issuing a first certificate Col 8 lines 25-30). Smith teaches that the certificate authority does not sign the certificate, (Col 5 lines 40-45 Fig 9).

“How PGP works” teaches that a PGP certificate contains the public key of the subject, long term identification information, and metadata (validity period), (Page 12). It is inherent that a certificate is invalid when the validity period expires. “How PGP works” does not teach a verifier with hashes.

Fischer teaches a system that has a verifier that maintains hashes of files in a security database. Fischer teaches that when files are presented they are scanned and a new hash

Art Unit: 2134

is computed to verify the file matches the hash stored in the database, (Col 12 line 63- Col 13 line 5).

It would have been obvious to one of ordinary skill in the art to modify the certificate system of Smith-PGP with the hash verifier of Fischer because the hash table verification would enhance the security of the system.

As per claims 2 and 14, "How PGP Works" teaches that the certificate has a time period, (Validity) (Page 12).

As per claims 6, 7, 8, 18, 19, and 20 it is well known in the art to use the hashing algorithms of MD5, and SHA1, which are collusion free hash algorithms.

**Claims 3, and 15, are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith US 6,651,166 in view of "How PGP works" in view of Fischer US 5,475,826 in view of Stallings "How to protect the company jewels"**

As per claims 3, and 15, the previous Smith-PGP-Fischer combination does not teach that the certificate may not need a time and date. Stallings teaches that the certificate is comprised without a expiration time (Page 3, paragraph 2, lines 1-2).

It would have been obvious to one of ordinary skill in the art to use the certificate of Smith -PGP-Fischer with the composition of Stallings because it allows more compressed certificates.

**Claims 4 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith US 6,651,166 in view of “How PGP works” in view of Fischer US 5,475,826 in view of Maruyama US 6,393,563**

As per claims 4 and 16, Smith -PGP-Fischer discloses a private key (Smith Fig 9).

Smith-PGP-Fischer does not disclose storing the private key on a smart card.

Maruyama disclose a private key may be stored on a smartcard, (Col 1 line 20, 53-56).

It would be obvious to modify the Smith -PGP-Fischer private key with Maruyama's smart card, because the smart card increases the security of key storage.

**Claims 5 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith US 6,651,166 in view of “How PGP works” in view of Fischer US 5,475,826 in view of Kausik US 6,263,446.**

As per claims 5 and 17, the previous Smith -PGP-Fischer combination does not disclose a software wallet.

Kausik discloses storing a private key in a software wallet, (Col 4 lines1-6).

It would be obvious to modify Smith-PGP-Fischer with Kausik's software wallet because the wallet increases the security of key storage.

**Claims 9, 21, 27, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith US 6,651,166 in view of "How PGP works" in view of Fischer US 5,475,826 in view of Gasser US 5,224,163.**

As per claims 9, 21, 27, and 28 the previous Smith-PGP-Fischer combination does not disclose that the certificate is revoked based on the validity of the long term information and public key.

Gasser discloses that if the key of the certificate is compromised, it is revoked, (Col 7 lines 5-9).

It would be obvious to one skilled in the art to modify Smith-PGP-Fischer certificate revocation with Gassers invalid key revocation, because a subject that used an invalid key would not be accepted.

**Claims 10, and 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith US 6,651,166 in view of "How PGP works" in view of Fischer US 5,475,826 in view of Micali US 5,793,868 in view of Boyle 6,212,636.**



As per claims 10 and 22, the previous Smith-PGP-Fischer combination does not disclose a revocation system involving hashes. Micali discloses a certificate revocation system where the certificate authority takes a hash of the certificates to be revoked, (Col 3 lines 18-23).

It would be obvious to one skilled in the art to modify Smith-PGP-Fischer revocation system with Micali's hashes, because hash's take less memory to store, and are well known for authentication properties in the art.

Boyle discloses that upon being notified that a certificate is revoked, that any data related to the certificate is erased from memory, (Col 21 line 59- 67).

It would be obvious to modify the Smith-PGP-Fischer-Micali combination above with Boyle's method of deletion, because a subject would not want to accidentally use a revoked certificate.

**Claims 11, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith US 6,651,166 in view of "How PGP works" in view of Fischer US 5,475,826 in view of Micali US 5,793,868 in view of Boyle 6,212,636 in view of Perlman US 5,687,235**

As per claims 11 and 23, the previous Smith-PGP-Fischer-Micali-Boyle combination does not teach the certificate authority marking a certificate as being invalid in a database.

Art Unit: 2134

Perlman teaches a certificate authority with a list of serial numbers of invalid certificates, and a CRL, (Col 6 lines 12-21).

It would have been obvious to one of ordinary skill in the art to use the CRL system of Perlman with the previous Smith-PGP-Fischer-Micali-Boyle combination because the CRL system improves the efficiency of an authentication exchange, (Perlman abstract).

**Claims 12, and 24, are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith US 6,651,166 in view of “How PGP works” in view of Fischer US 5,475,826 in view of Micali US 5,793,868 in view of Boyle 6,212,636 in view of Gasser US 5,224,163.**

As per claims 12 and 24, the previous Smith-PGP-Fischer-Micali-Boyle combination does not disclose deleting the certificate from the database once it has been revoked.

Gasser discloses a certificate authority (GNS) deletes the revoked certificate, (Col 7 lines 5-10).

It would be obvious to one skilled in the art to modify the Smith-PGP-Fischer-Micali-Boyle combination with Gasser’s deletion method because the certificates are no longer useful.

***Conclusion***


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jaques Louis Jaques can be reached on (571)272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher J. Brown

6/28/06



JACQUES LOUIS JACQUES  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100